Amendments to the claims:

1. (presently amended) A method of enforcing security policies in a data access system, said data access system having data access management software in program memory, said method comprising:

defining a first condition;

upon occurrence of said first condition, placing a rule into data access management software in said data access system, said rule testing for a second condition and precluding an action if said second condition is present, said rule being stored remotely and only loaded into program memory for the duration of said first condition, said rule being placed into data access management for an amount of time that differs from an amount of time for which a user is logged on.

2. (original) The method of claim 1 wherein said condition is effectuation of a first transaction by a user and said second action is the effectuation of a related transaction by the same user.

3. (previously amended) The method of claim 1 wherein said first condition is effectuation of a first transaction by a first user in a particular role, and said action is the effectuation of a second transaction and said second condition is that a specified user is associated with said second action.

4. (previously amended) The method of claim 3 wherein the first user and the specified user are different.

5. (previously amended) The method of claim 2, further comprising eliminating said rule from said data access management software immediately upon rescinding of said condition.

6. (previously amended) The method of claim 2 wherein a user attempting to effectuate said second action is informed of said first condition or said second condition and advised automatically that said second action is prohibited.

7. (presently amended) The method of claim 2 wherein said first action is the ordering of goods or services and said second action is the payment for such goods or services and said second condition is the user attempting such payment is the same user ordering said goods or ~~servies~~services.

8. (presently amended) Apparatus for enforcing security policies to increase security of data access management software, said apparatus comprising:

a file of rules, said rules only being applicable to prevent specified data transactions by a first user upon the effectuation of a specified action by said first user, said specified action occurring after said user logs on to said data access management software and being defined by one or more transactions a user may effectuate;

software for recognizing that said first user has effected said specified action, and

means for reading said file, locating said rules to prevent said specified data transactions, and, upon occurrence of said specified action of said first user, integrating said rules into said data access management software such that said specified data transactions are prohibited, wherein said rules are not integrated with said data access management software prior to said occurrence of said specified action.

9. (original) Apparatus of claim 8 wherein further comprising means for eliminating the rule from the data access management software at the conclusion of a predetermined time or upon a predetermined condition.

10. (presently amended) A method of enforcing confidentiality in the form of a wall comprising the steps of:

storing at least one rule that prohibits a known party from accessing specified information in a database or file of a data access system if a first specified condition occurs after said known party has

logged on to said data access system;

upon a first specified condition occurring, modifying data access management software to include a rule that prohibits a known party from accessing specified information in a database or file;

said first specified condition being indicative of said known party having knowledge of a particular set of information; and

upon a second specified condition occurring, removing said rule from the data access management software and storing said rule for future use, said specified second condition indicating that said knowledge is no longer sensitive.

11. (original) The method of claim 10 wherein said rule is generated from a template rule.

12. (original) The method of claim 11 wherein said known party is defined as any individual engaged in a predetermined role.

13. (previously presented) The method of claim 10 wherein said known party is notified of the occurrence of said second condition.

14. (original) The method of claim 13 wherein said notification is via email.

15. (original) The method of claim 10 wherein said knowledge is no longer sensitive because it has been made public or because a predetermined time has passed.

16. (original) The method of claim 1 wherein said rule is generated from a template rule.

17. (previously presented) The method of claim 10 wherein some other individual, not the known party, is notified of the occurrence of said second condition.

18. (previously presented) The method of claim 17 wherein said notification is via e-mail.

19. (previously presented) The method of claim 11 wherein some other individual, not the known party, is notified of the occurrence of said second condition.

20. (previously presented) The method of claim 19 wherein said notification is via e-mail.

21. (cancelled)

22. (previously presented) The method of claim 11 wherein another individual, not the known party, is notified when the known party attempts the prohibited second action more than once.

23. (previously presented) The method of claim 10 wherein another individual, not the known party, is notified when the known party attempts to access said specified information in the database more than once.

24. (previously presented) The method of claim 23 wherein the notification is via e-mail.

25. (original) The method of claim 22 wherein the notification is via e-mail.

26. (previously presented) The method of claim 23 wherein said another individual is the users manager or supervisor.

27. (previously presented) The method of claim 23 wherein said another individual is responsible for data security.

28. (previously presented) The method of claim 22 wherein said another individual is the users manager or supervisor.

29. (previously presented) The method of claim 22 wherein said another individual is responsible for data security.

30. (previously presented) The apparatus of claim 9 wherein the eliminated rule is saved in an audit log.

31. (previously presented) The method of claim 10 wherein the removed rule is saved in an audit log.

32. (previously presented) The method of claim 1 wherein the rule is not loaded until a specified user logs on to the system.

33. (previously presented) The method of claim 1 wherein the rule is only tested for a specified user.

34. (previously presented) The method of claim 10 wherein the rule is not loaded until a specified user logs on to the system.

35. (previously presented) The method of claim 10 wherein the rule is only tested for a specified user.

36. (previously presented) The method of claim 3 wherein the rule is not loaded until a user in a specified role logs on to the system.

37. (previously presented) The method of claim 3 wherein the rule is only tested for a user in a specified role.

38. (previously presented) The method of claim 12 wherein the rule is not loaded until a user in a specified role logs on to the system.

39. (previously presented) The method of claim 12 wherein the rule is only tested for a user in a specified role.

40. (original) The method of claim 1 wherein the security policy is separation of duties.

41. (original) The method of claim 1 wherein the security policy is compliance to regulation.

42. (original) The method of claim 1 wherein the security policy is privacy of data.

43. (previously presented) The method of claim 23 wherein said another individual is a computer process.

44. (previously presented) The method of claim 22 wherein said another individual is a computer process.

45. (previously presented) The method of claim 1 wherein said rule is generated upon occurrence of said condition.

46. (previously presented) The apparatus of claim 8 further comprising means for generating said rules upon occurrence of said specified action of said first user.

47. (previously presented) The method of claim 10 wherein said rule is generated upon occurrence of said first specified condition.